CHAPTER 1

BASIC PROGRAM POLICY AND AUTHORITIES

1-1 BASIC POLICY

1. This regulation establishes the Department of the Navy (DON) Personnel Security Program (PSP) under the authority of Executive Order (E.O.) 12968, Access to Classified Information, reference (a) and E.O. 10450, Security Requirements for Government Employees, and in compliance with Department of Defense (DoD) 5200.2-R, DoD Personnel Security Program Regulation, January 1987 (NOTAL) reference (b).

2. The objective of the PSP is to authorize initial and continued access to classified information and/or initial and continued assignment to sensitive duties to those persons whose loyalty, reliability and trustworthiness are such that entrusting the persons with classified information or assigning the persons to sensitive duties is clearly consistent with the interests of national security. Additionally, the PSP ensures that no final unfavorable personnel security determination will be made without compliance with all procedural requirements.

1-2 AUTHORITY

1. The Secretary of the Navy (SECNAV) is responsible for establishing and maintaining a Personnel Security Program in compliance with the provisions of E.O.s, public laws, National Security Council guidance, DoD regulation and other security directives regarding trustworthiness standards and the protection of classified information.

2. The SECNAV has designated the Chief of Naval Operations, Special Assistant for Naval Investigative Matters and Security, (CNO (N09N)), who functions primarily as the Director, Naval Criminal Investigative Service (NCIS), as the senior security official of the DON. CNO (N09N) is responsible for ensuring that the DON has an effective PSP and for complying with all directives issued by higher authority.

1-3 NATIONAL AUTHORITIES FOR SECURITY MATTERS

1. **The President** of the United States (U.S.), bears executive responsibility for the security of the Nation which includes the authority to classify information and limit access thereto for the protection of the national defense and foreign relations of the United States. Standards for the classification and

safeguarding of national security information are detailed in E.O. 12958 and standards for personnel receiving access thereto are detailed in E.O. 12968.

2. **The National Security Council (NSC)** provides overall policy guidance on information and personnel security matters.

3. **The Director of the Information Security Oversight Office (ISOO),** has the responsibility for issuing directives as necessary to implement E.O. 12958 and provides guidance regarding the Classified Information Nondisclosure Agreement, Standard Form (SF) 312.

4. **The Security Policy Board (SPB)** is an interagency organization co-chaired by the Deputy Secretary of Defense and the Director of Central Intelligence created by the President to consider, coordinate, and recommend to the President, through the NSC, uniform standards, policies and procedures governing classified information and personnel security, to be implemented and applicable throughout the Federal Government.

5. **The Attorney General of the United States** upon request from the head of an agency or the Director, ISOO, interprets E.O. provisions in response to questions arising from implementation.

6. **The Office of Personnel Management (OPM)** is responsible for oversight and implementation of E.O. 10450, which prescribes security requirements (including investigations) for federal government employment.

7. **The Director of Central Intelligence (DCI),** as the chairman of the National Foreign Intelligence Board (NFIB), issues instructions in the form of DCI directives or policy statements affecting intelligence policies and activities. The DCI is charged by 50 U.S.C. Section 403(g), National Security Act of 1947, with protecting intelligence sources and methods.

8. **The Federal Bureau of Investigation (FBI)** is the primary internal security agency of the Government with jurisdiction over investigative matters which include espionage, sabotage, treason and other subversive activities.

9. **The Secretary of the Navy (SECNAV)** is the Department of the Navy agency head responsible under E.O. 12968 for establishing and maintaining an effective program to ensure that access to classified information by each DON employee is clearly consistent with the interests of national security.

1-4 DEPARTMENT OF DEFENSE SECURITY PROGRAM AUTHORITIES

1. **The Assistant Secretary of Defense for Command, Control, Communications and Intelligence (ASD(C3I))** is the senior DoD official charged by the Secretary of Defense with responsibility for development of policies and procedures governing information and personnel security policy programs. The Deputy Assistant Secretary of Defense, Security and Information Operations (DASD(S&IO)) issues DoD 5200.1-R, Information Security Program Regulation (NOTAL), and DoD 5200.2-R, Personnel Security Program Regulation, reference (b) (NOTAL).

2. **The Deputy Under Secretary of Defense for Policy Support DUSD(PS)** administers international security policy and performs administrative support to the Secretary of Defense who is designated the United States Security Authority for NATO (USSAN). The USSAN implements security directives issued by the North Atlantic Treaty Organization (NATO) and oversees the Central U.S. Registry (CUSR), with the Department of the Army as executive agency.

3. **The National Security Agency (NSA)** provides centralized coordination and direction for signals intelligence and communications security for the Federal Government. The DON contributes to these efforts primarily through the Commander, Naval Security Group Command (COMNAVSECGRU). The Director, NSA is authorized by the Secretary of Defense to prescribe procedures or requirements, in addition to those in DoD regulations, for Sensitive Compartmented Information (SCI) and communications security (COMSEC). The authority to lower any COMSEC security standard within the DoD rests with the Secretary of Defense.

4. **The Defense Intelligence Agency (DIA)** coordinates the intelligence efforts of the Army, Navy and Air Force and is responsible for implementation of standards and operational management of SCI for the DoD. The Director, DIA is the Senior Official of the Intelligence Community (SOIC) for DoD and is a member of the NFIB.

5. **The Defense Security Service (DSS)** conducts personnel security investigations for the DoD (with the exception of those investigations conducted by OPM and investigations conducted overseas). DSS additionally administers the National Industrial Security Program (NISP) as the executive agency and provides security training for employees of defense contractors and for DoD military and civilian personnel. DSS components include:

a. **The National Computer Center (NCC)**, created to support the DSS Strategic Implementation Plan, is involved with automation projects such as the Electronic Personnel Security Questionnaire (EPSQ) and Defense Clearance and Investigations Index (DCII) enhancements.

b. **The DSS Operations Center - Baltimore**, is the operations center controlling personnel security investigations conducted by DSS.

c. **The Deputy Director, Industrial Security** manages the DoD implementation of the NISP through regional Cognizant Security Offices throughout the operating centers in the Continental United States (CONUS) and the Offices of Industrial Security International in locations overseas.

d. **The DSS Operations Center - Columbus**, grants personnel security clearances to individuals in private industry (contractors) who need access to classified information in order to perform their jobs and responds to requests for information regarding contractor personnel security clearance applications.

e. **The Security Research Center** performs research and analysis to improve security programs.

f. **The Office of Mission Training (OMT)** provides job training to DSS investigative agents and other security training previously provided by the Department of Defense Security Institute (DoDSI) to DoD contractors and DoD employees.

1-5 DEPARTMENT OF THE NAVY SECURITY PROGRAM MANAGEMENT

1. **The Secretary of the Navy (SECNAV).** SECNAV is responsible for implementing a PSP in compliance with the provisions of E.O.'s, public laws, and directives issued by the NRC, DOE, DoD, DCI, and other agencies.

2. **The Special Assistant for Naval Investigative Matters and Security, Office of the Chief of Naval Operations (CNO (N09N))/Director, Naval Criminal Investigative Service (DIRNCIS).** The SECNAV has designated CNO (N09N)/DIRNCIS as the **DON senior agency security official** under reference (a). The Assistant for Information and Personnel Security (CNO (N09N2))/Deputy Assistant Director, Information and Personnel Security Programs (NCIS-21) provides staff support for these functions and responsibilities.

a. CNO (N09N) is responsible to the SECNAV for establishing, directing, and overseeing an effective DON PSP and for

implementing and complying with all directives issued by higher authority. This responsibility includes:

(1) Formulating policies and procedures, issuing directives, monitoring, inspecting, and reporting on the status of administration of the PSP in the Navy and Marine Corps.

(2) Establishing and maintaining continuing security awareness, training, and education programs to ensure effective implementation of reference (a).

(3) Cooperating with other agencies to achieve practical, consistent, and effective adjudicative training and guidelines.

(4) Establishing procedures to prevent unnecessary access to classified information, including procedures to establish need to know before access is authorized and to limit the number of persons granted access to classified information to the minimum consistent with operational needs and security requirements.

b. CNO (N09N) is also responsible for establishing, administering, and overseeing the DON Information Security Program (ISP) and issuing information security policy and procedures through reference (d).

3. **The Director, Department of the Navy Central Adjudication Facility (DON CAF)** reports directly to DIRNCIS and is the personnel security adjudicative determination authority for all DON personnel.

4. **The Director of Naval Intelligence (CNO (N2))**, as the Senior Official of the Intelligence Community (SOIC) for the DON, is responsible for administering the Navy's SCI program. **The Office of Naval Intelligence (ONI)**, is responsible for the security management and implementation of SCI programs. **The Director, Security Directorate (ONI-5)**, as Special Security Officer/Special Activities Officer for the DON (SSO Navy), is responsible for guidance and instruction on matters concerning the security, control and use of SCI.

5. **The Commander, Naval Security Group Command (COMNAVSECGRU)**, is responsible for the security and administration of SCI programs within the Department's cryptologic community.

6. **The Deputy Chief of Naval Operations (CNO (N89)), Special Programs Division**, is responsible for security policy and procedures for SAPs established under Special Access Program Oversight Committee (SAPOC) authority.

7. **The Director, Navy International Programs Office (Navy IPO),** is assigned the authority to approve or disapprove routine requests for access to or transfer of DON technical data or disclosure of DON classified or sensitive unclassified information to other nations in accordance with national disclosure policy.

1-6 SPECIAL PROGRAMS

1. The security requirements for access to information classified as Confidential, Secret or Top Secret normally provide sufficient protection. Any program requiring additional security protection, handling measures, reporting procedures or formal access lists is considered a special program.

2. Most special programs requiring additional security measures have been established by authorities outside the DON. Although the requirements for these programs are included in this regulation, these programs are implemented and governed in the DON by the following instructions: OPNAVINST C5510.101D, NATO Security Procedures (U) (NOTAL); OPNAVINST S5511.35K, Policy for Safeguarding the Single Integrated Operational Plan (SIOP) (U) (NOTAL); SECNAVINST 5510.35, Nuclear Weapon Personnel Reliability Program (PRP); SECNAVINST 5312.12B, Selection of Department of the Navy Military and Civilian Personnel and Contractor Employees for Assignment to Presidential Support Activities; OPNAVINST C8126.1A, Navy Nuclear Weapon Security (U) (NOTAL); DoD Directive 5210.2 of 12 January 1978, Access to and Dissemination of Restricted Data (NOTAL), and the Navy Department Supplement to DoD S-5105.21-M-1 of 8 Mar 95 (NOTAL) for the protection of SCI.

1-7 SPECIAL ACCESS PROGRAMS (SAP)

Programs requiring security measures in addition to those requirements for the protection of Top Secret, Secret or Confidential classified information which are established by and within the Department of Defense are referred to as DoD SAPs. A DoD SAP must be authorized by the Secretary of Defense or by the Deputy Secretary of Defense and is governed by DoD Directive 0-5205.7, Special Access Program (SAP) Policy of 13 Jan 1997 (NOTAL), DoD Instruction 0-5205.11, Management, Administration, and Oversight of DoD Special Access Programs (SAPs) of 1 Jul 97 (NOTAL); DoD 5220.22-M, National Industrial Security Program Operating Manual of January 1995 (NOTAL); and SECNAVINST S5460.3B, Control of Special Access Programs within the Department of the Navy (U) (NOTAL). The Deputy Chief of Naval Operations (CNO (N89)) receives and reviews requests for SAPs from DON requesters and the Under Secretary of the Navy must

formally approve the establishment of each SAP in coordination with the Deputy Secretary of Defense.

1-8 APPLICABILITY

1. This regulation applies to all regular and reserve military members of the Navy and Marine Corps; civilian personnel employed by, hired on a contractual basis by, or serving in an advisory/consultant capacity to the DON whether on a permanent, temporary or part-time basis, and whether or not compensated from appropriated or non-appropriated funds; and applicants selected for sensitive positions, or persons accepted for consideration for enlistment or appointment (military), or other persons covered by contract or other legal agreement.

2. This regulation establishes coordinated policies for personnel security matters. It incorporates policies provided in references (a) through (c) and other directives bearing on personnel security. This is the controlling regulation for implementation and maintenance of the DON PSP. Personnel security provisions incorporated in other departmental directives must comply with these policies and procedures.

3. This regulation provides minimum requirements. Commanding officers may choose to impose more stringent requirements on their command or on their subordinate commands; however, they may not establish requirements that impact on commands that are not their subordinate commands. Commanding officers may not establish requirements that are contradictory to this regulation.

4. Commanding officers are responsible for compliance with and implementation of this regulation within their commands. Personnel are individually responsible for compliance with this regulation.

1-9 COMBAT OPERATIONS

Security requirements may be modified as necessary to meet local conditions in combat or combat-related operations. In these circumstances, follow the provisions of this regulation as closely as possible. Exercises are not combat-related operations. This exception does not apply to regularly scheduled training exercises or operations.

1-10 WAIVERS

1. When a commanding officer finds that fulfilling the requirements of this regulation will result in an untenable

sacrifice of operating efficiency, or when there are other good and sufficient reasons, a waiver of a specific requirement may be requested from the Chief of Naval Operations (N09N2) via the administrative chain of command.

2. Each request for waiver must give the reason why the requirement cannot be met and describe the alternative procedures or protection to be provided.

1-11 COMMANDING OFFICER

"Commanding officer" is used throughout this regulation as a generic term for the head of an organizational entity and includes commander, commanding general, director, officer in charge, etc. Responsibilities assigned to the commanding officer by this regulation may be delegated unless specifically prohibited. "Command" is used as a generic term for the organizational entity and includes ship, laboratory, facility, activity, unit, squadron, etc.

1-12 GUIDANCE

1. Requests for guidance or clarification of this regulation may be addressed formally or informally to the Chief of Naval Operations (N09N2), 716 Sicard Street, SE, Washington, DC 20388-5381. For telephone inquiries, the Security Action Line (with a recorder for after-hours calls) may be reached at DSN 288-8856, commercial (202) 433-8856. Send facsimile requests to (202) 433-8849. The CNO homepage at www.navysecurity.navy.mil provides policy updates, security awareness items and other instructional materials.

2. Definitions of terms used in this regulation are listed in appendix A.

3. Acronyms used throughout this regulation are listed in appendix B.